Information Technology Security Charter

1. Mission

The Information Security Office of the North Carolina Office of Information Technology Services (ISO) exists to assure the availability, integrity, and confidentiality of information, as appropriate. The office's main objectives include development and implementation of policies standards and technical measures to prevent security incidents. The office also responds to information technology security incidents when prevention methods fail.

2. Scope

This charter applies to all employees, contractors, and third parties having access to state resources either on-site or through remote access to state information systems.

3. Duties of the staff responsible for various information technology security functions

All individuals subject to this Charter are responsible for ensuring that state information assets are used as intended for official state business, ensuring that information is not improperly disclosed to any unauthorized persons and that information assets are not modified without proper authorization, or otherwise endangered. Any employee or contractor involved in selecting, purchasing, or operating computer system or application software or hardware is responsible for ensuring that approved and published security policies and standards can be effectively implemented for that system or application

A. The State of North Carolina Chief Information Officer (State CIO) is responsible for:

- Developing and administering a comprehensive long range plan for the proper management of the state's information technology assets.
- Establishing, reviewing, and updating statewide information technology security standards, policies, and procedures.
- Reviewing agency security standards to determine whether those standards meet statewide security requirements.
- Including information security assessment results in the statewide information technology plan.
- Estimating costs to implement adequate information technology security measures.
- Assuming direct responsibility for providing information technology security for any state agency that fails to adhere to state security standards.
- Reporting on information technology security matters to the Information Technology Advisory Board and the Joint Legislative Oversight Committee.
- Reviewing information technology projects for appropriate risk mitigation and information technology security planning.
- Recording and tracking information security incidents and sharing cyber security incident information with the Office of the State Auditor and the Office of the State Attorney General as appropriate.

B. The State of North Carolina Deputy State Chief Information Officer (Deputy CIO) is responsible for operational implementation of the state's information security program.

C. The State of North Carolina Chief Information Security Officer (State CISO) is responsible for ensuring that appropriate security controls are defined and for assisting state agencies in their efforts to implement adequate information technology security measures. The State CISO is responsible for:

- Proposing security policy, standards, and guidelines to the State CIO as they apply to the State's distributed information technology assets.
- Managing the Information Security Office (ISO) to implement the statewide information security standards, policies, procedures, architecture, and objectives set by the State CIO and the Deputy CIO.
- Reviewing existing security standards and practices among the various State agencies to determine whether those standards and practices are in force and meet enterprise-wide security requirements.
- Acting as the Chief Information Security Officer for an agency, should the State Chief Information Officer assume direct responsibility of providing for the information technology security of any State agency that fails to adhere to security standards.

D. The Information Security Office develops and maintains information security standards, policies, and procedures, and identifies and implements measures to mitigate risks.

- The Infrastructure Security team supports and monitors the security of the state's information technology infrastructure.
- The Threat Management and Incident Response team provides security alerts and warnings, oversees response to cyber security incidents, and manages the statewide cyber incident response plan.
- The Information Security Consulting and Support Services team provides expert assistance to agencies on information technology security matters.

E. State agency and department management must evaluate all stored information, applications, and information systems to determine the appropriate controls required to protect the information assets on the basis of its criticality to the business, value to the state and its citizens, and potential value to outside interests. Agency managers are responsible for:

- Providing information technology security information to the State CIO as requested.
- Forecasting agency information security needs and projected costs.
- Designating an agency security liaison and appropriate information security support staff.
- Responding to agency cyber security incidents and reporting information security incidents to the ISO.
- Compliance with statewide security standards, policies, procedures, architectures, and other legal requirements.
- Implementing information security measures within their agency.
- Managing information security risks.
- Including information security measures in agency project plans.
- Mitigation of information security vulnerabilities and threats.
- Maintaining cyber incident response plans and business continuity plans.

4. Violation reporting and escalation

Persons identified in this charter must report violations of the published security charter, as well as policies and standards to their agency manager. If the violation does not appear to be resolved in a timely manner, the State Chief Information Security Officer must be notified by the person observing the violation. All verified information security incidents must be reported within 24 hours to the Information Security Office. Ongoing operational information systems that deviate from statewide information security standards, policies, procedures, and architectures must be reported to the information security office.

5. The scope of contingency and disaster recovery

A serious incident that can prevent the State of North Carolina and/or any of its agencies from continuing normal business operations can happen at any time. A business continuity plan protecting information assets from both natural and manmade disasters must be documented and tested on an annual basis. The State CIO is responsible for overseeing such plans and managing the statewide testing process.

6. Legal Authority

N.C.G.S. Chapter 147, Article 3D.